

What's new in Elastic Stack

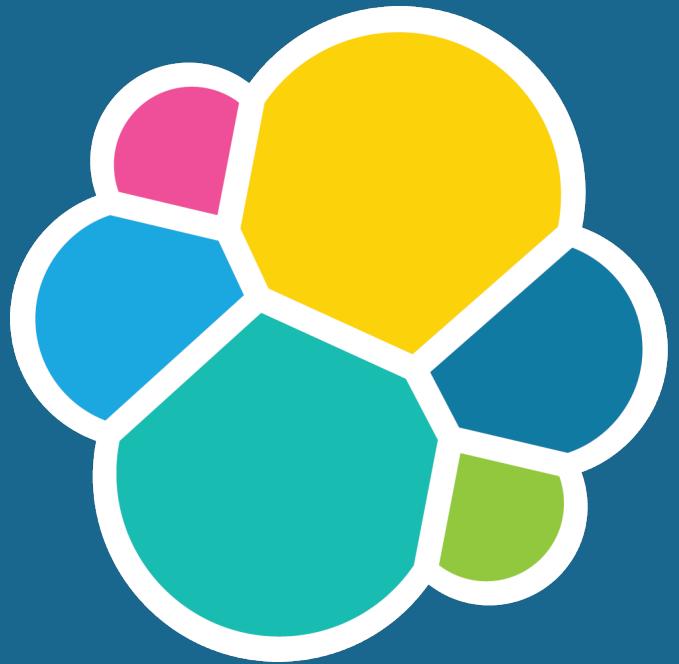
7.x

Emanuil Tolev

@emanuil_tolev



@emanuil_tolev



elastic

Community Engineer



@emanuil_tolev

Lots of things!

Search

Data management

Security



@emanuil_tolev

Search



elastic

@emanuil_tolev

Adaptive replica selection

Ever tried to load balance ES?



@emanuil_tolev

Skipping refreshes on idle shards

(wut?)



elastic

@emanuil_tolev

Default to 1 shard

Time for a tiny bit of theory



elastic

@emanuil_tolev

Cross-cluster search



@emanuil_tolev

A little older feature, not really
7.x, but this is an important
improvement to it. Anybody
using it already?

Zen2

**Quorum setting (minimum_master_nodes)
gone!**



@emanuil_tolev

Index Lifecycle Management is GA



@emanuil_tolev

any users?

- ^ Imagine filebeat continuously writing to an index. We want to roll over 50 GB or age 30d ago, and delete after 90d.
- ^ So what does that look like? I'd like to do you a full demo but not today.

```
PUT _ilm/policy/datasream_policy
{
  "policy": {
    "phases": {
      "hot": {
        "actions": {
          "rollover": {
            "max_size": "50GB",
            "max_age": "30d"
          }
        }
      },
      "delete": {
        "min_age": "90d",
        "actions": {
          "delete": {}
        }
      }
    }
  }
}
```



@emanuil_tolev

deleted 90 days after it is
rolled over

```
PUT _template/datasream_template
{
  "index_patterns": [ "datasream-*" ],
  "settings": {
    "number_of_shards": 1,
    "number_of_replicas": 1,
    "index.lifecycle.name": "datasream_policy",
    "index.lifecycle.rollover_alias": "datasream"
  }
}
```



@emanuil_tolev

created a policy, now to apply
it to an index

```
PUT datastream-000001
{
  "aliases": {
    "datastream": {
      "is_write_index": true
    }
  }
}
```



@emanuil_tolev

bootstrap - policy will then roll over, create new indices and move old ones off as defined
^ requires that the name ends in a number

```
GET dastream-*/_ilm/explain
```

```
// aaaand:  
{  
  "indices": {  
    "dastream-000001": {  
      "index": "dastream-000001",  
      "managed": true,  
      "policy": "dastream_policy",  
      "phase": "hot",           <-- 1  
      "action": "rollover",     <-- 2  
      "step": "attempt-rollover", <-- 3  
      "phase_execution": {  
        "policy": "dastream_policy",  
        "phase_definition": {  
          // ... 50 GB or max age 30 days, etc.  
        }  
      }  
    }  
  }  
}
```



@emanuil_tolev

cut out some of it but you can
see what's up
^ phase, action, step
^ the rest spits our own
settings back at us

"datastream": alias for searching and writing



@emanuil_tolev

search across all managed
indices and write to the
appropriate one
^ cool huh

SQL is now GA



@emanuil_tolev

what? Yes, the SQL adapter to
a NoSQL datastore.

^ now with geo features
allowing you to access the ES
geo queries! OpenGIS

How to use it?

- the usual REST endpoints
- the ES SQL command line interface
 - the JDBC driver
 - the ODBC driver



@emanuil_tolev

```
POST /_sql?format=txt
{
  "query": "SELECT * FROM library ORDER BY page_count DESC LIMIT 5"
}
```

author	name	page_count	release_date
Peter F. Hamilton	Pandora's Star	768	2004-03-02T00:00:00.000Z
Vernor Vinge	A Fire Upon the Deep	613	1992-06-01T00:00:00.000Z
Frank Herbert	Dune	604	1965-06-01T00:00:00.000Z
Alastair Reynolds	Revelation Space	585	2000-03-15T00:00:00.000Z
James S.A. Corey	Leviathan Wakes	561	2011-06-02T00:00:00.000Z



@emanuil_tolev

still can't quite believe the eng
effort SQL to NoSQL :D

```
$ ./bin/elasticsearch-sql-cli https://sql_user:strongpassword@some.server:9200
```

```
sql> SELECT * FROM library WHERE page_count > 500 ORDER BY page_count DESC;
```

author	name	page_count	release_date
Peter F. Hamilton	Pandora's Star	768	1078185600000
Vernor Vinge	A Fire Upon the Deep	613	7073568000000
Frank Herbert	Dune	604	-1447200000000
Alastair Reynolds	Revelation Space	585	9530784000000
James S.A. Corey	Leviathan Wakes	561	1306972800000



@emanuil_tolev

much more traditional. User,
pass, server all optional.

Data frames

**In the spirit of connecting with nostalgia,
basically pivot tables**

Summarise one index into another one



@emanuil_tolev

Pandas in Python has this concept and apparently the 2 map quite well, but I haven't tried it.

^ This is a huge feature, meriting its own talk or two. Check it out if pivot tables sound interesting.

Search as you type field type

`search_as_you_type` **in the mapping**



@emanuil_tolev

text-like field; out-of-the-box support for as-you-type completion use case

^ creates a series of subfields that are analyzed to index terms that can be efficiently matched by a query that partially matches the entire indexed text value.

^ Both prefix completion (i.e matching terms starting at the beginning of the input) and infix completion (i.e. matching terms at any position within the input) are supported.

Flattened field type

flattened **in the mapping**



@emanuil_tolev

Rare terms agg

"order" : { "_count" : "asc" } on a Terms
agg



elastic

@emanuil_tolev

JSON logging



@emanuil_tolev

we talk a lot about structured
logging

^ if you use the stack to
monitor ES itself, you can now
do so more easily

vector similarity search



@emanuil_tolev

not my specialty

- ^ word2vec and CNNs understand text similarity in this way
- ^ this makes it closer and easier to the mental models used in certain ML projects
- ^ considered the next hot thing in search engine features

TLS intra-cluster encryption now free



elastic

@emanuil_tolev

RBAC (Role Based Access Control) also free



elastic

@emanuil_tolev

a free SIEM



@emanuil_tolev

security information and event
management
^ absolutely enormous - lots of
vendors offer one, we integrate
it with the rest of the stack and
it's free

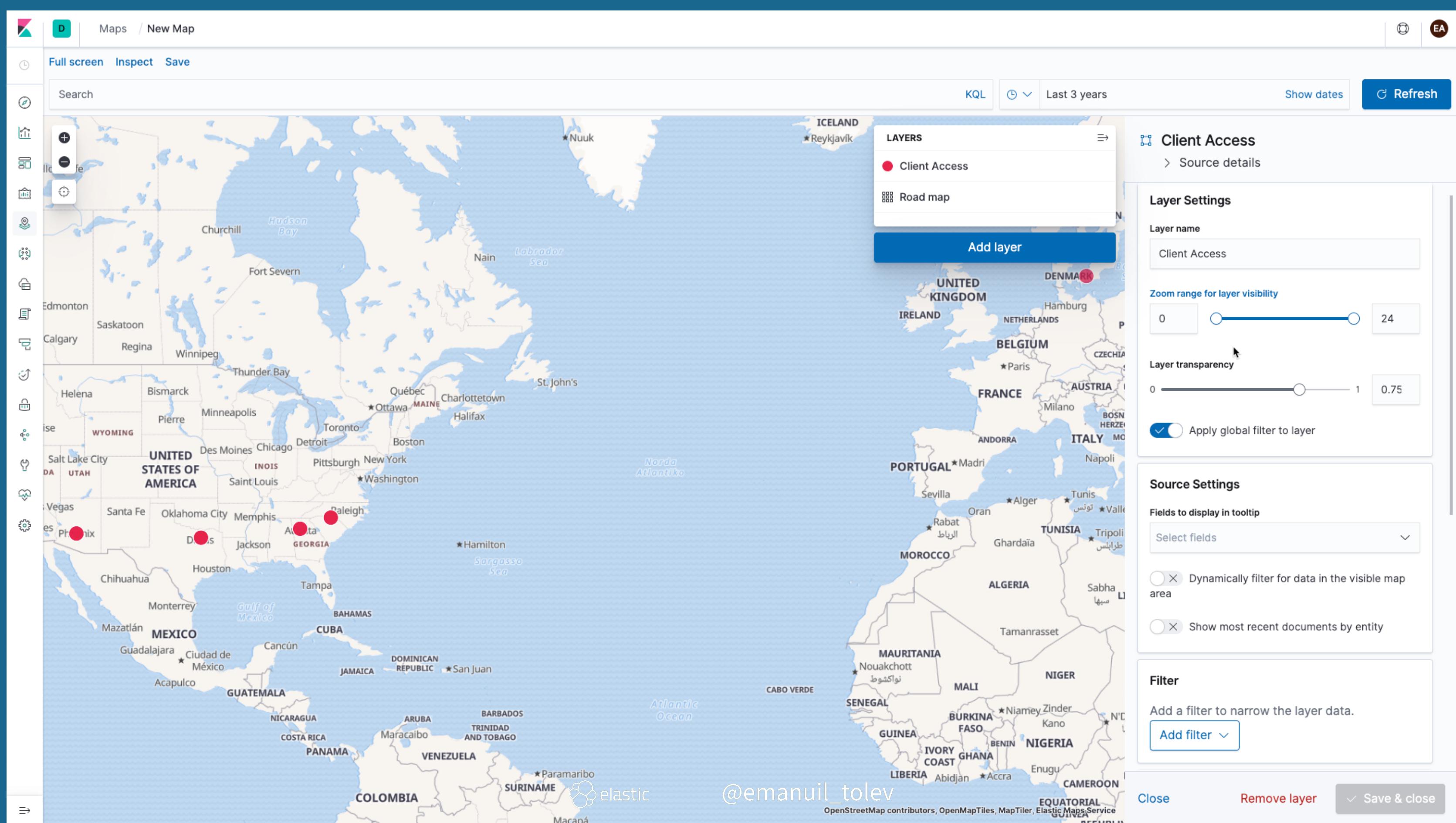
APM

.NET is now GA

**Interesting maps integration for the JS
Real User Monitoring (RUM)**



@emanuil_tolev



RUM with Maps integration
^ would quite like to do APM demos,
it's awesome how it integrates with
logging, machine learning and other
features. A powerful platform.
Important to me personally too -
burnout ops.

Manchester!

GOVERNMENT DAY on Wed September 11, 9am until 5pm

[https://events.elastic.co/
20190911elasticgovernmentday](https://events.elastic.co/20190911elasticgovernmentday)

KUBERNETES WORKSHOP on Thu September 12, 9am until 1pm

<http://events.elastic.co/20190912monitoringkubernetes>



@emanuil_tolev

More free educational events for Manchester

Manchester is a priority city. Looking at **ML, security, on top of Logging, APM, Observability**

→ Host, speak or just stay informed:
genevieve.loriant@elastic.co or me,
etolev@elastic.co

→ BBLs!



@emanuil_tolev

You're a priority for us. ML, security, on top of Logging, APM, Observability.

- ^ If you want to host, speak or just come:
genevieve.loriant@elastic.co or me
- ^ Also your account team if you're a customer.
- ^ If you're not I'm happy to come and do a Brown Bag Lunch with one of your tech teams.

Questions?

Emanuil Tolev

@emanuil_tolev

etolev@elastic.co



@emanuil_tolev